INTERNATIONAL CYBERSECURITY AND DIGITAL FORENSICS ACADEMY

Assignment Title: Static Malware Analysis-Investigating a suspicious malware

Course Code: ACI803 Malware Analysis for Cybercrime

Student Name: Ahtisham Tanveer

Student ID: 2025/ACI/9979

Programme: Advance Cybercrime Investigations

Instructor Name: Aminu Idris

Date of Submission: 09/14/2025

STUDENT ID CARD

AHTISHAM TANVEER
2025/ACI/9979
CYBERCRIME INVESTIGATIONS

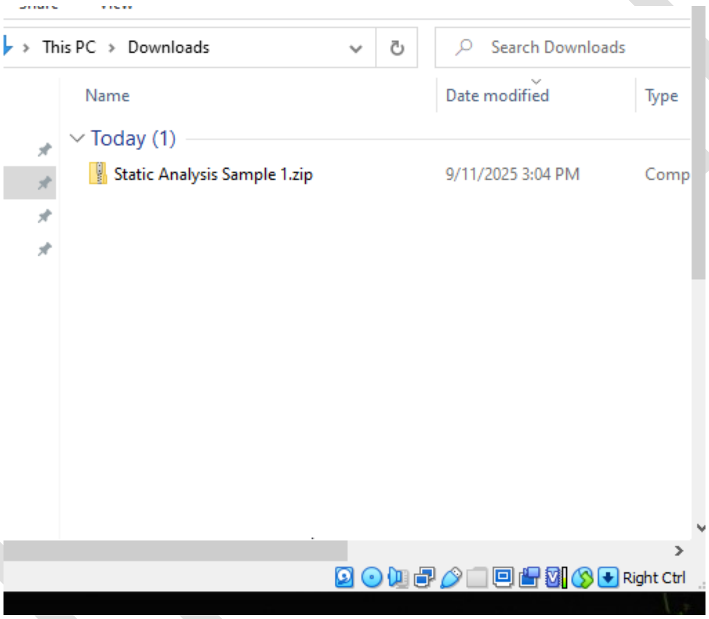
Exp Date: **November, 2025**

1. Executive Summary

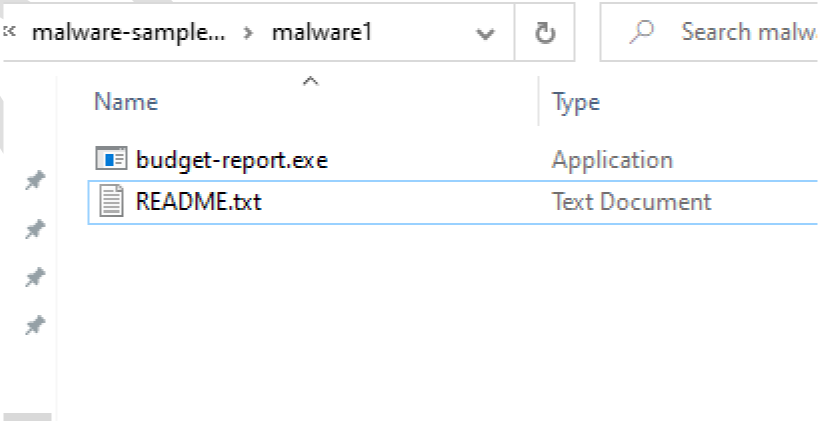
During this investigation, a suspicious Windows executable was analyzed using static malware analysis techniques inside a controlled FLARE VM environment. The sample was discovered on a workstation involved in a financial fraud case and had initially evaded antivirus detection.

Analysis revealed that the file is a **packed 32-bit Windows Portable Executable (PE)** designed to conceal its functionality. The binary makes use of memory allocation, process manipulation, and networking-related APIs, suggesting capabilities such as process injection and command-and-control (C2) communication. Strings and import table analysis identified possible indicators of compromise (IOCs), including suspicious API calls and references consistent with credential theft or banking malware.

Overall, the evidence supports the assessment that this executable is **malicious**, most likely a banking trojan or loader associated with financial crime campaigns.



Name	Date modified	Type
Today (1)		
Static Analysis Sample 1.zip	9/11/2025 3:04 PM	Comp



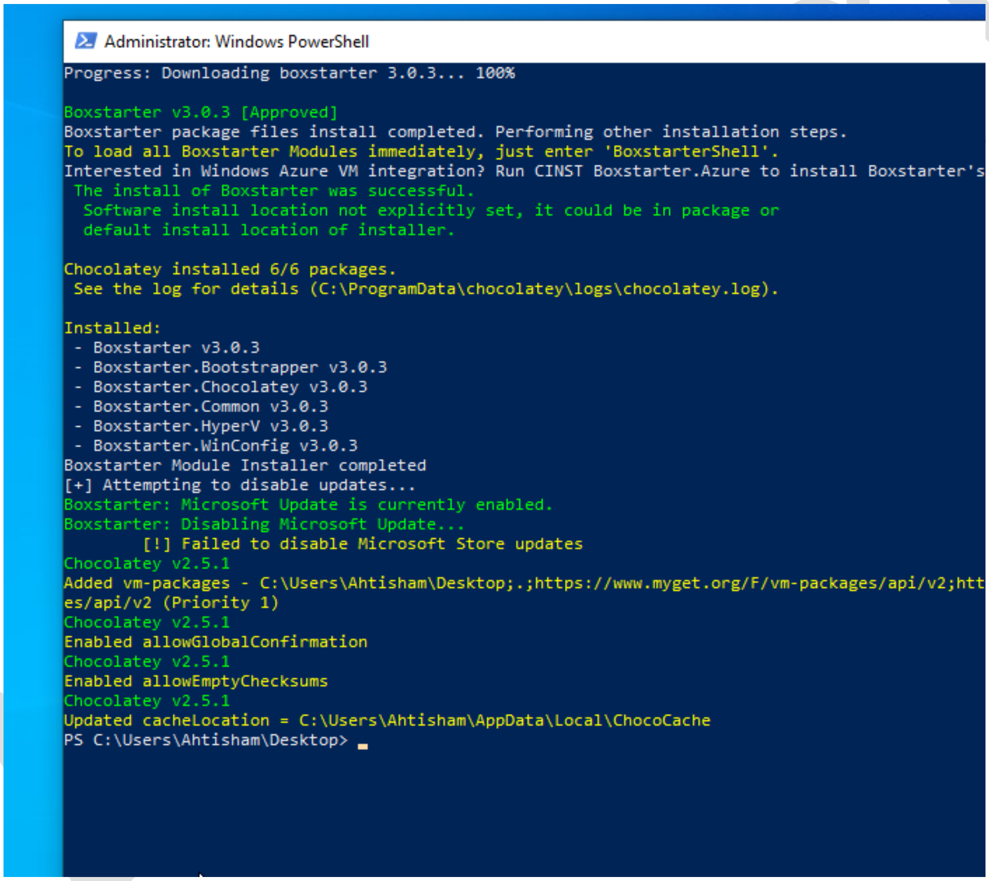
Name	Type
budget-report.exe	Application
README.txt	Text Document

Lab Environment – Using FLARE VM:

The virtual machine environment was configured using **FLARE VM**, which leverages **Boxstarter** and **Chocolatey** as automation tools for installing and managing the analysis utilities.

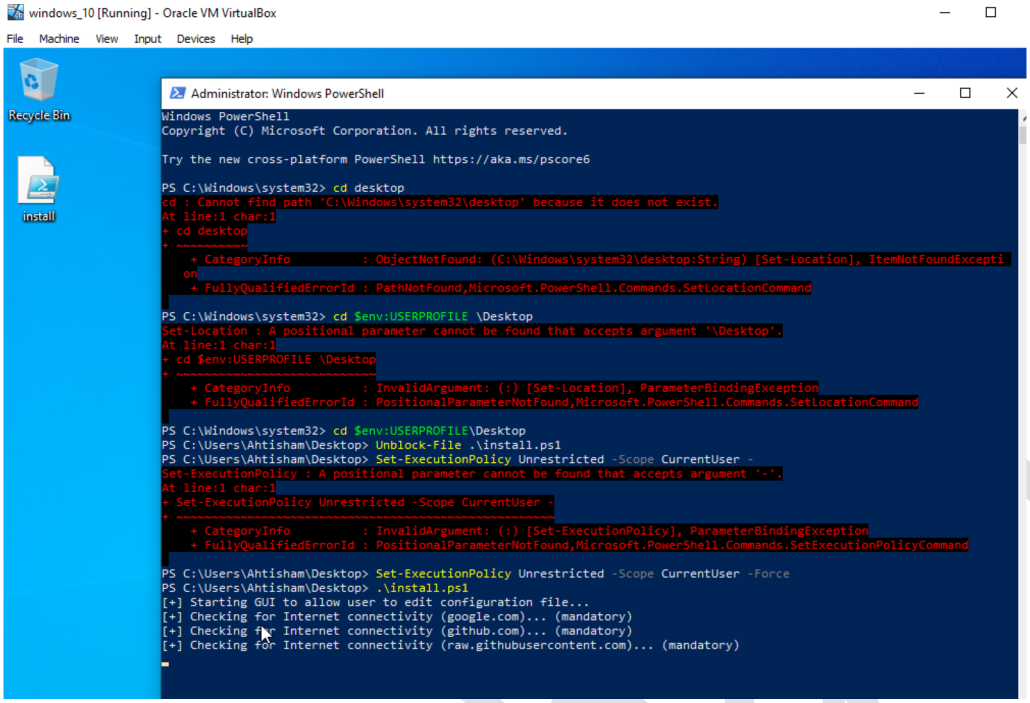
- **Boxstarter** was used to automate initial configuration of the VM.
- **Chocolatey** served as the package manager for installing malware analysis tools such as PEStudio, Detect It Easy, IDA Free, and Strings.

This ensured that the environment was consistent, reproducible, and contained all required analysis tools without manual setup errors.



Administrator: Windows PowerShell

```
Progress: Downloading boxstarter 3.0.3... 100%

Boxstarter v3.0.3 [Approved]
Boxstarter package files install completed. Performing other installation steps.
To load all Boxstarter Modules immediately, just enter 'BoxstarterShell'.
Interested in Windows Azure VM integration? Run CINST Boxstarter.Azure to install Boxstarter's
 The install of Boxstarter was successful.
  Software install location not explicitly set, it could be in package or
  default install location of installer.

Chocolatey installed 6/6 packages.
 See the log for details (C:\ProgramData\chocolatey\logs\chocolatey.log).

Installed:
 - Boxstarter v3.0.3
 - Boxstarter.Bootstrapper v3.0.3
 - Boxstarter.Chocolatey v3.0.3
 - Boxstarter.Common v3.0.3
 - Boxstarter.HyperV v3.0.3
 - Boxstarter.WinConfig v3.0.3
Boxstarter Module Installer completed
[+] Attempting to disable updates...
Boxstarter: Microsoft Update is currently enabled.
Boxstarter: Disabling Microsoft Update...
        [!] Failed to disable Microsoft Store updates
Chocolatey v2.5.1
Added vm-packages - C:\Users\Ahtisham\Desktop;.;https://www.myget.org/F/vm-packages/api/v2;htt
es/api/v2 (Priority 1)
Chocolatey v2.5.1
Enabled allowGlobalConfirmation
Chocolatey v2.5.1
Enabled allowEmptyChecksums
Chocolatey v2.5.1
Updated cacheLocation = C:\Users\Ahtisham\AppData\Local\ChocoCache
PS C:\Users\Ahtisham\Desktop> _
```


windows_10 [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Recycle Bin
install
Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> cd desktop
cd : Cannot find path 'C:\Windows\system32\desktop' because it does not exist.
At line:1 char:1
+ cd desktop
+ ~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (C:\Windows\system32\desktop:String) [Set-Location], ItemNotFoundExcepti
   on
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SetLocationCommand

PS C:\Windows\system32> cd $env:USERPROFILE \Desktop
Set-Location : A positional parameter cannot be found that accepts argument '\Desktop'.
At line:1 char:1
+ cd $env:USERPROFILE \Desktop
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidArgument: (:) [Set-Location], ParameterBindingException
    + FullyQualifiedErrorId : PositionalParameterNotFound,Microsoft.PowerShell.Commands.SetLocationCommand

PS C:\Windows\system32> cd $env:USERPROFILE\Desktop
PS C:\Users\Ahtisham\Desktop> Unblock-File .\install.ps1
PS C:\Users\Ahtisham\Desktop> Set-ExecutionPolicy Unrestricted -Scope CurrentUser -
Set-ExecutionPolicy : A positional parameter cannot be found that accepts argument '-'.
At line:1 char:1
+ Set-ExecutionPolicy Unrestricted -Scope CurrentUser -
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidArgument: (:) [Set-ExecutionPolicy], ParameterBindingException
    + FullyQualifiedErrorId : PositionalParameterNotFound,Microsoft.PowerShell.Commands.SetExecutionPolicyCommand

PS C:\Users\Ahtisham\Desktop> Set-ExecutionPolicy Unrestricted -Scope CurrentUser -Force
PS C:\Users\Ahtisham\Desktop> .\install.ps1
[+] Starting GUI to allow user to edit configuration file...
[+] Checking for Internet connectivity (google.com)... (mandatory)
[+] Checking for Internet connectivity (github.com)... (mandatory)
[+] Checking for Internet connectivity (raw.githubusercontent.com)... (mandatory)
```

2. Analysis Section

Countering errors and solutions, while executing a malware:

Defender Exclusion

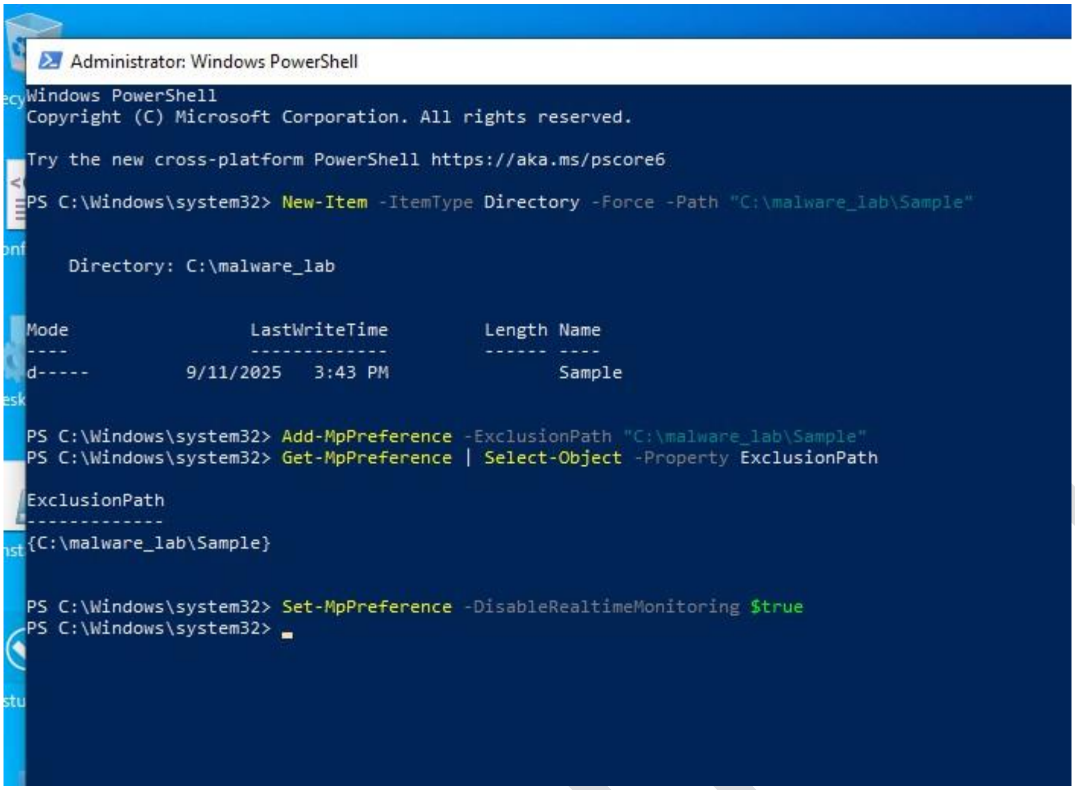
Microsoft Defender kept deleting the malware sample during analysis. To stop this, we excluded only the analysis folder from Defender scans so the file would stay intact without disabling protection system-wide.

Disabling Real-Time Protection

Even with the exclusion, Defender was still aggressive. We briefly turned off real-time monitoring so tools like PEStudio and Detect It Easy could access the file.

Restoring Security

After finishing the analysis, we turned Defender back on and removed the exclusion. This returned the VM to a safe state and reduced any risk of infection.

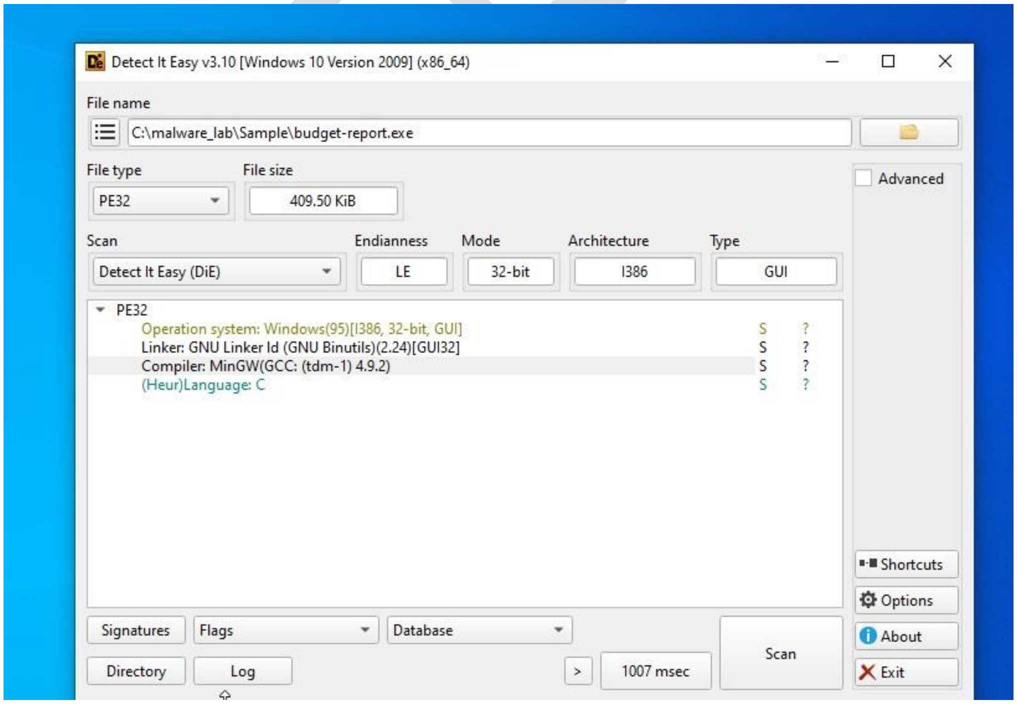


Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> New-Item -ItemType Directory -Force -Path "C:\malware_lab\Sample"


    Directory: C:\malware_lab


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         9/11/2025   3:43 PM                Sample


PS C:\Windows\system32> Add-MpPreference -ExclusionPath "C:\malware_lab\Sample"
PS C:\Windows\system32> Get-MpPreference | Select-Object -Property ExclusionPath

ExclusionPath
-------------
{C:\malware_lab\Sample}


PS C:\Windows\system32> Set-MpPreference -DisableRealtimeMonitoring $true
PS C:\Windows\system32> _
```

Task 1: Basic File Identification

Tools Used: Detect It Easy (DIE), PEStudio



Detect It Easy v3.10 [Windows 10 Version 2009] (x86_64)

File name: C:\malware_lab\Sample\budget-report.exe

File type: PE32

File size: 409.50 KiB

□ Advanced

Scan: Detect It Easy (DiE)

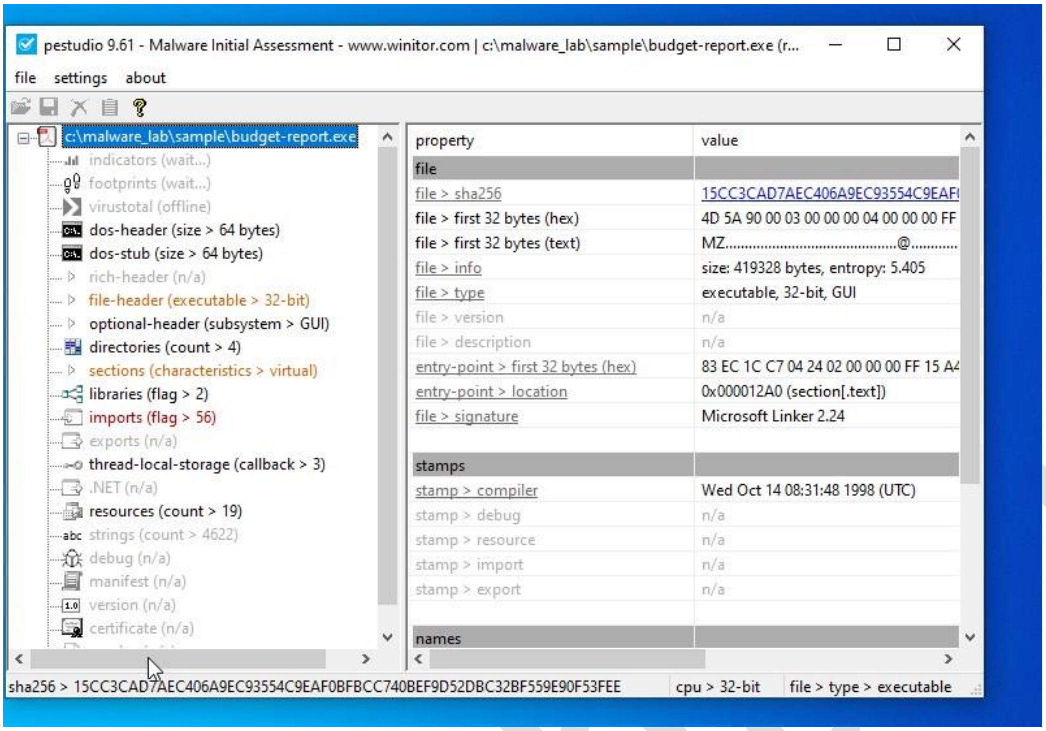
Endianness: LE

Mode: 32-bit

Architecture: I386

Type: GUI

```
PE32
    Operation system: Windows(95)[I386, 32-bit, GUI]      S   ?
    Linker: GNU Linker ld (GNU Binutils)(2.24)[GUI32]      S   ?
    Compiler: MinGW(GCC: (tdm-1) 4.9.2)                    S   ?
    (Heur)Language: C                                      S   ?
```

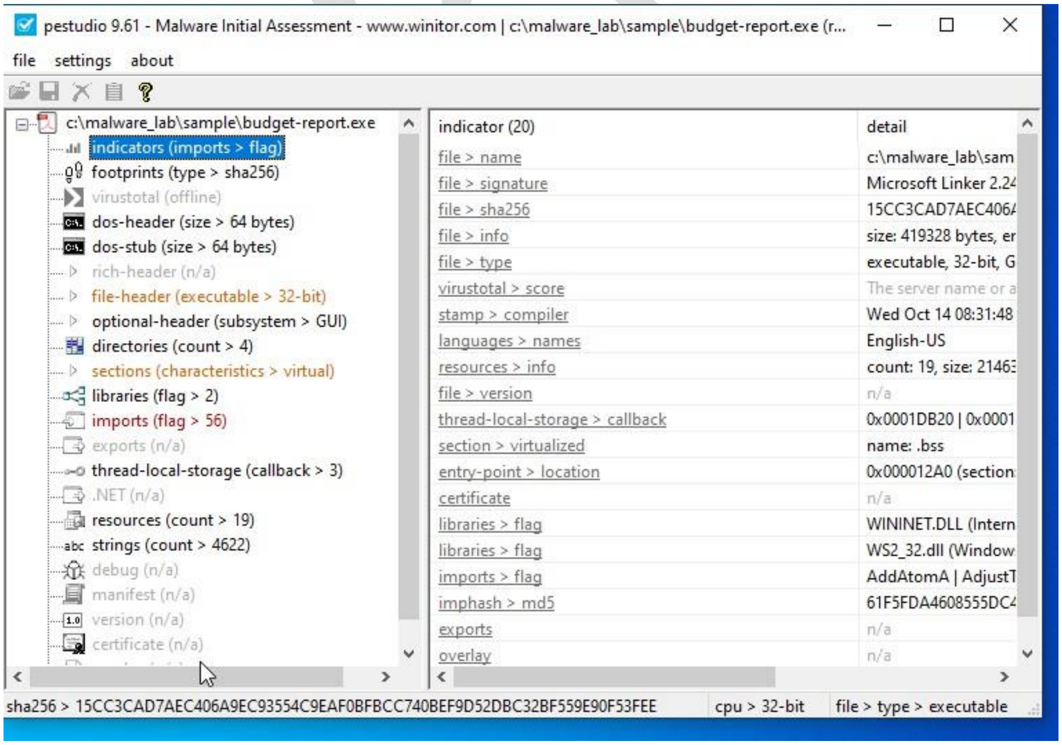


pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\malware_lab\sample\budget-report.exe (r...

```
c:\malware_lab\sample\budget-report.exe
    indicators (wait...)
    footprints (wait...)
    virustotal (offline)
    dos-header (size > 64 bytes)
    dos-stub (size > 64 bytes)
    rich-header (n/a)
    file-header (executable > 32-bit)
    optional-header (subsystem > GUI)
    directories (count > 4)
    sections (characteristics > virtual)
    libraries (flag > 2)
    imports (flag > 56)
    exports (n/a)
    thread-local-storage (callback > 3)
    .NET (n/a)
    resources (count > 19)
    strings (count > 4622)
    debug (n/a)
    manifest (n/a)
    version (n/a)
    certificate (n/a)
```

property	value
file	
file > sha256	15CC3CAD7AEC406A9EC93554C9EAF
file > first 32 bytes (hex)	4D 5A 90 00 03 00 00 00 04 00 00 00 FF
file > first 32 bytes (text)	MZ..@...........
file > info	size: 419328 bytes, entropy: 5.405
file > type	executable, 32-bit, GUI
file > version	n/a
file > description	n/a
entry-point > first 32 bytes (hex)	83 EC 1C C7 04 24 02 00 00 00 FF 15 A4
entry-point > location	0x000012A0 (section[.text])
file > signature	Microsoft Linker 2.24
stamps	
stamp > compiler	Wed Oct 14 08:31:48 1998 (UTC)
stamp > debug	n/a
stamp > resource	n/a
stamp > import	n/a
stamp > export	n/a
names	

sha256 > 15CC3CAD7AEC406A9EC93554C9EAF0BFBCC740BEF9D52DBC32BF559E90F53FEE   cpu > 32-bit   file > type > executable

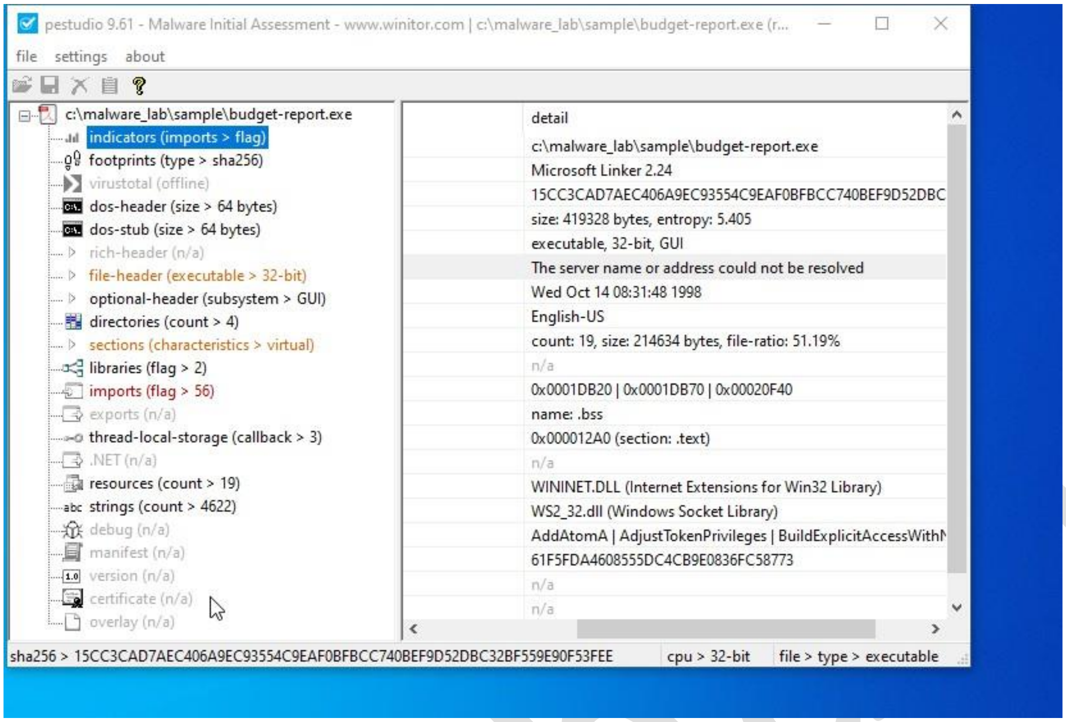


pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\malware_lab\sample\budget-report.exe (r...

```
c:\malware_lab\sample\budget-report.exe
    indicators (imports > flag)
    footprints (type > sha256)
    virustotal (offline)
    dos-header (size > 64 bytes)
    dos-stub (size > 64 bytes)
    rich-header (n/a)
    file-header (executable > 32-bit)
    optional-header (subsystem > GUI)
    directories (count > 4)
    sections (characteristics > virtual)
    libraries (flag > 2)
    imports (flag > 56)
    exports (n/a)
    thread-local-storage (callback > 3)
    .NET (n/a)
    resources (count > 19)
    strings (count > 4622)
    debug (n/a)
    manifest (n/a)
    version (n/a)
    certificate (n/a)
```

indicator (20)	detail
file > name	c:\malware_lab\sam
file > signature	Microsoft Linker 2.24
file > sha256	15CC3CAD7AEC406A
file > info	size: 419328 bytes, er
file > type	executable, 32-bit, G
virustotal > score	The server name or a
stamp > compiler	Wed Oct 14 08:31:48
languages > names	English-US
resources > info	count: 19, size: 21463
file > version	n/a
thread-local-storage > callback	0x0001DB20 | 0x0001
section > virtualized	name: .bss
entry-point > location	0x000012A0 (section
certificate	n/a
libraries > flag	WININET.DLL (Intern
libraries > flag	WS2_32.dll (Window
imports > flag	AddAtomA | AdjustT
imphash > md5	61F5FDA4608555DC4
exports	n/a
overlay	n/a

sha256 > 15CC3CAD7AEC406A9EC93554C9EAF0BFBCC740BEF9D52DBC32BF559E90F53FEE   cpu > 32-bit   file > type > executable



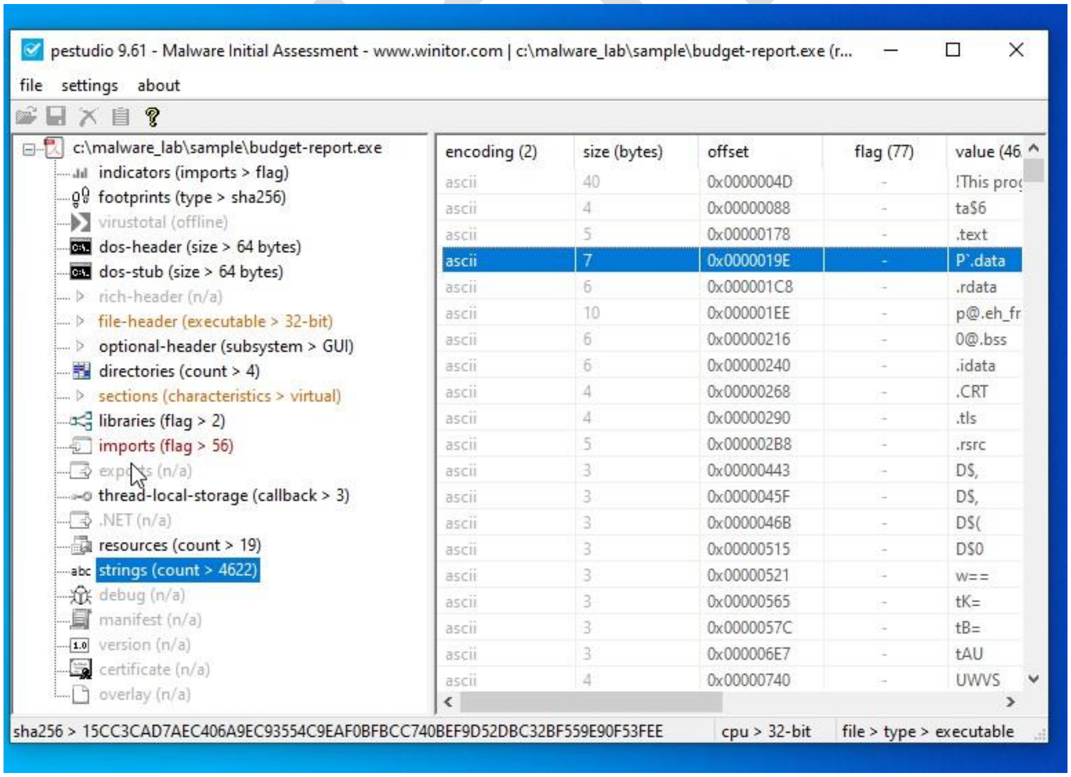
pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\malware_lab\sample\budget-report.exe (r...

- c:\malware_lab\sample\budget-report.exe
  - indicators (imports > flag)
  - footprints (type > sha256)
  - virustotal (offline)
  - dos-header (size > 64 bytes)
  - dos-stub (size > 64 bytes)
  - rich-header (n/a)
  - file-header (executable > 32-bit)
  - optional-header (subsystem > GUI)
  - directories (count > 4)
  - sections (characteristics > virtual)
  - libraries (flag > 2)
  - imports (flag > 56)
  - exports (n/a)
  - thread-local-storage (callback > 3)
  - .NET (n/a)
  - resources (count > 19)
  - strings (count > 4622)
  - debug (n/a)
  - manifest (n/a)
  - version (n/a)
  - certificate (n/a)
  - overlay (n/a)

detail
c:\malware_lab\sample\budget-report.exe
Microsoft Linker 2.24
15CC3CAD7AEC406A9EC93554C9EAF0BFBCC740BEF9D52DBC
size: 419328 bytes, entropy: 5.405
executable, 32-bit, GUI
The server name or address could not be resolved
Wed Oct 14 08:31:48 1998
English-US
count: 19, size: 214634 bytes, file-ratio: 51.19%
n/a
0x0001DB20 | 0x0001DB70 | 0x00020F40
name: .bss
0x000012A0 (section: .text)
n/a
WININET.DLL (Internet Extensions for Win32 Library)
WS2_32.dll (Windows Socket Library)
AddAtomA | AdjustTokenPrivileges | BuildExplicitAccessWithN
61F5FDA4608555DC4CB9E0836FC58773
n/a
n/a

sha256 > 15CC3CAD7AEC406A9EC93554C9EAF0BFBCC740BEF9D52DBC32BF559E90F53FEE | cpu > 32-bit | file > type > executable

Task 2: Strings Analysis

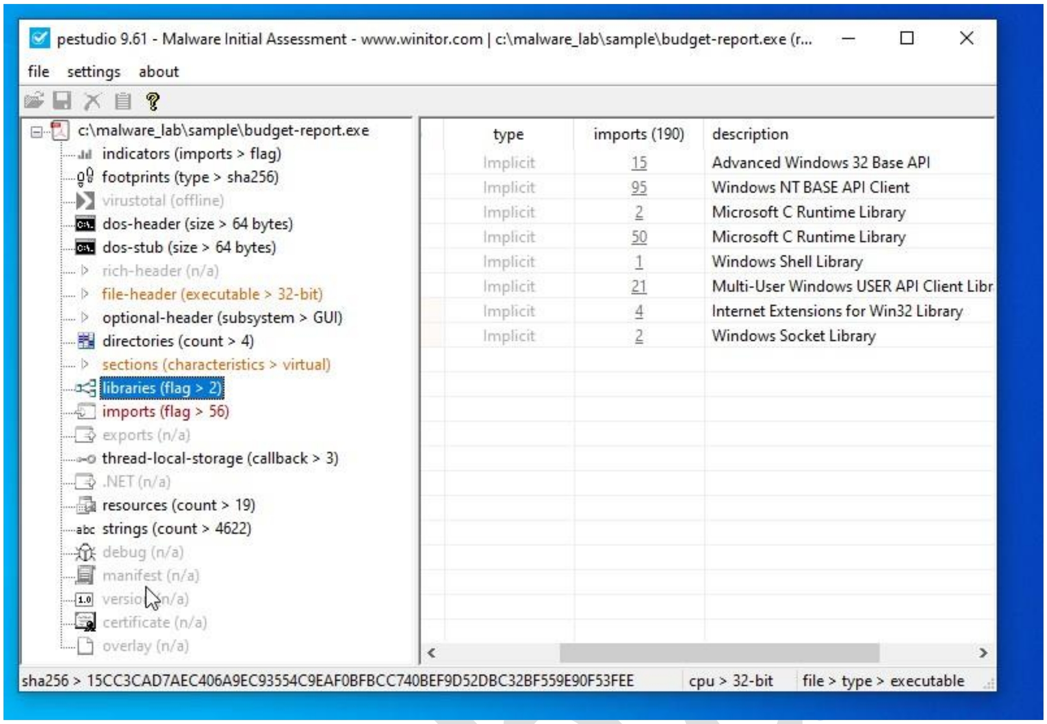


pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\malware_lab\sample\budget-report.exe (r...

- c:\malware_lab\sample\budget-report.exe
  - indicators (imports > flag)
  - footprints (type > sha256)
  - virustotal (offline)
  - dos-header (size > 64 bytes)
  - dos-stub (size > 64 bytes)
  - rich-header (n/a)
  - file-header (executable > 32-bit)
  - optional-header (subsystem > GUI)
  - directories (count > 4)
  - sections (characteristics > virtual)
  - libraries (flag > 2)
  - imports (flag > 56)
  - exports (n/a)
  - thread-local-storage (callback > 3)
  - .NET (n/a)
  - resources (count > 19)
  - strings (count > 4622)
  - debug (n/a)
  - manifest (n/a)
  - version (n/a)
  - certificate (n/a)
  - overlay (n/a)

encoding (2)	size (bytes)	offset	flag (77)	value (46
ascii	40	0x0000004D	-	!This prog
ascii	4	0x00000088	-	ta$6
ascii	5	0x00000178	-	.text
ascii	7	0x0000019E	-	P`.data
ascii	6	0x000001C8	-	.rdata
ascii	10	0x000001EE	-	p@.eh_fr
ascii	6	0x00000216	-	0@.bss
ascii	6	0x00000240	-	.idata
ascii	4	0x00000268	-	.CRT
ascii	4	0x00000290	-	.tls
ascii	5	0x000002B8	-	.rsrc
ascii	3	0x00000443	-	D$,
ascii	3	0x0000045F	-	D$,
ascii	3	0x0000046B	-	D$(
ascii	3	0x00000515	-	D$0
ascii	3	0x00000521	-	w==
ascii	3	0x00000565	-	tK=
ascii	3	0x0000057C	-	tB=
ascii	3	0x000006E7	-	tAU
ascii	4	0x00000740	-	UWVS

sha256 > 15CC3CAD7AEC406A9EC93554C9EAF0BFBCC740BEF9D52DBC32BF559E90F53FEE | cpu > 32-bit | file > type > executable



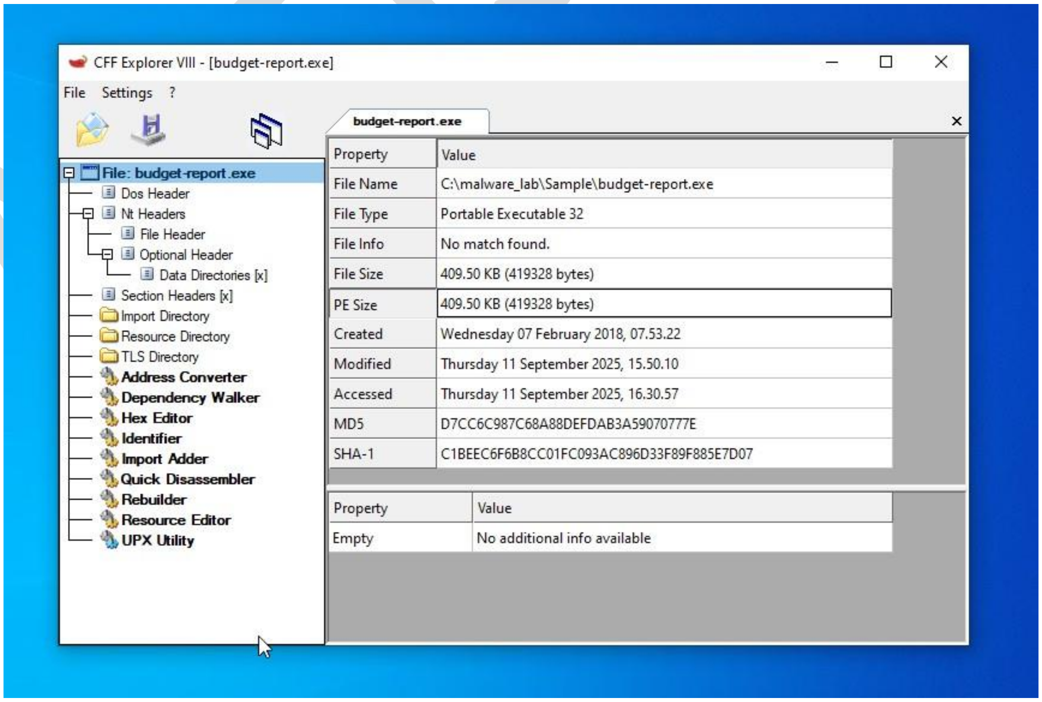
pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\malware_lab\sample\budget-report.exe (r...

```
c:\malware_lab\sample\budget-report.exe
    indicators (imports > flag)
    footprints (type > sha256)
    virustotal (offline)
    dos-header (size > 64 bytes)
    dos-stub (size > 64 bytes)
    rich-header (n/a)
    file-header (executable > 32-bit)
    optional-header (subsystem > GUI)
    directories (count > 4)
    sections (characteristics > virtual)
    libraries (flag > 2)
    imports (flag > 56)
    exports (n/a)
    thread-local-storage (callback > 3)
    .NET (n/a)
    resources (count > 19)
    strings (count > 4622)
    debug (n/a)
    manifest (n/a)
    version (n/a)
    certificate (n/a)
    overlay (n/a)
```

type	imports (190)	description
Implicit	15	Advanced Windows 32 Base API
Implicit	95	Windows NT BASE API Client
Implicit	2	Microsoft C Runtime Library
Implicit	50	Microsoft C Runtime Library
Implicit	1	Windows Shell Library
Implicit	21	Multi-User Windows USER API Client Libr
Implicit	4	Internet Extensions for Win32 Library
Implicit	2	Windows Socket Library

sha256 > 15CC3CAD7AEC406A9EC93554C9EAF0BFBCC740BEF9D52DBC32BF559E90F53FEE   cpu > 32-bit   file > type > executable

Task 3: PE Header and Section Review

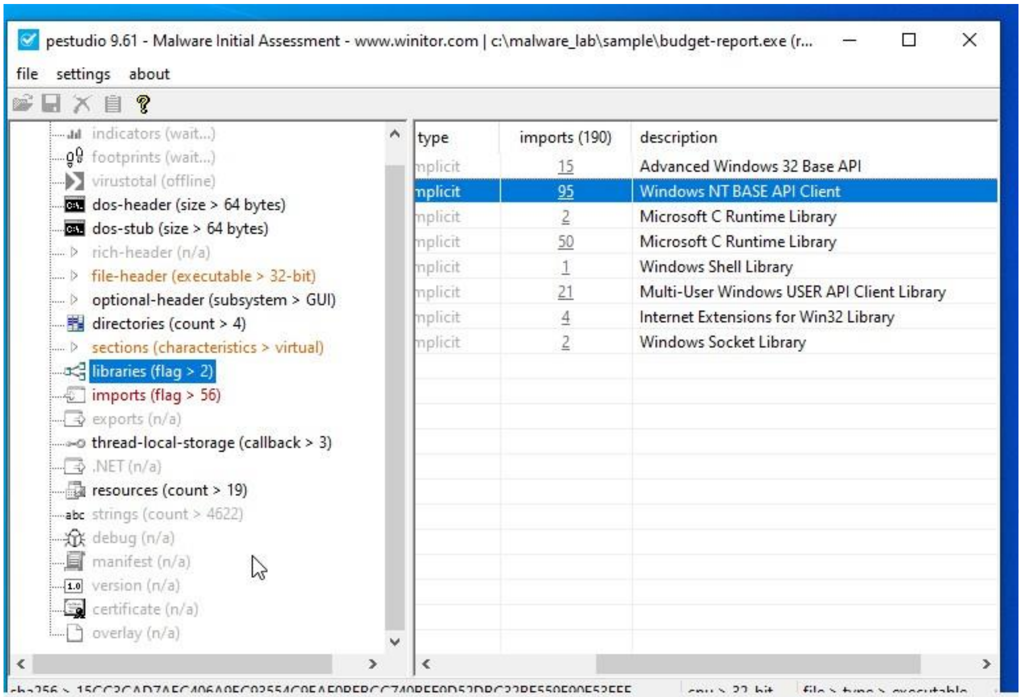


CFF Explorer VIII - [budget-report.exe]

```
File: budget-report.exe
    Dos Header
    Nt Headers
        File Header
        Optional Header
            Data Directories [x]
    Section Headers [x]
    Import Directory
    Resource Directory
    TLS Directory
    Address Converter
    Dependency Walker
    Hex Editor
    Identifier
    Import Adder
    Quick Disassembler
    Rebuilder
    Resource Editor
    UPX Utility
```

Property	Value
File Name	C:\malware_lab\Sample\budget-report.exe
File Type	Portable Executable 32
File Info	No match found.
File Size	409.50 KB (419328 bytes)
PE Size	409.50 KB (419328 bytes)
Created	Wednesday 07 February 2018, 07.53.22
Modified	Thursday 11 September 2025, 15.50.10
Accessed	Thursday 11 September 2025, 16.30.57
MD5	D7CC6C987C68A88DEFDAB3A59070777E
SHA-1	C1BEEC6F6B8CC01FC093AC896D33F89F885E7D07

Property	Value
Empty	No additional info available

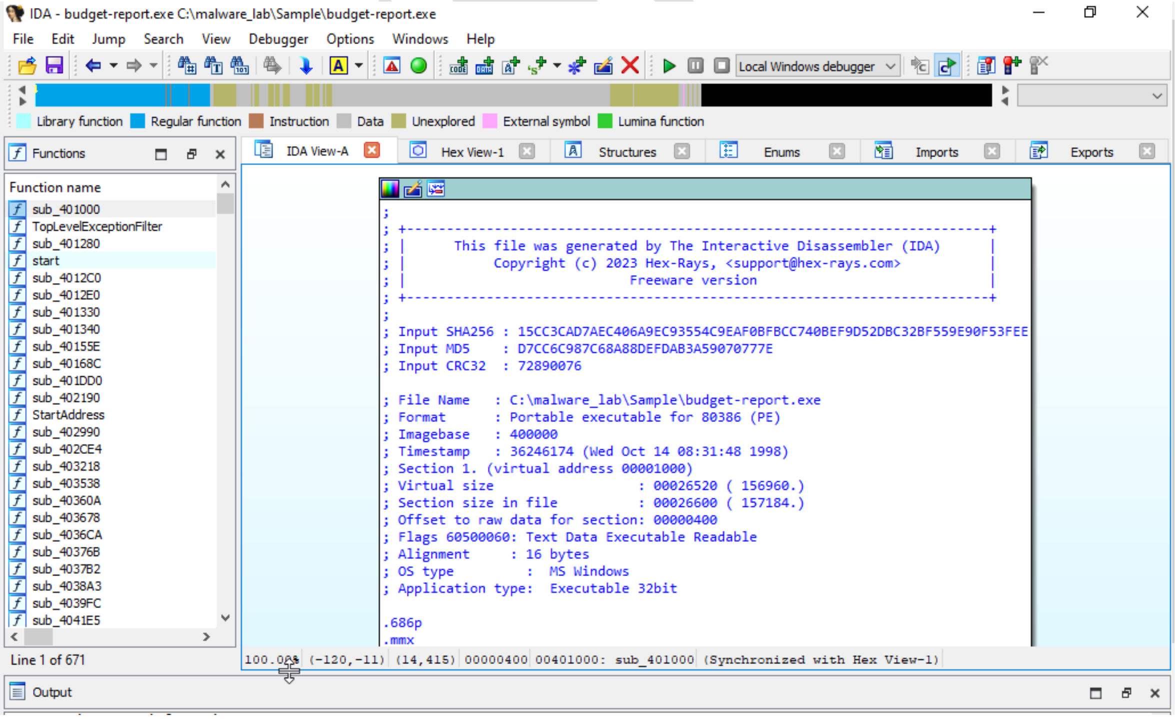


pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\malware_lab\sample\budget-report.exe (r...

- indicators (wait...)
- footprints (wait...)
- virustotal (offline)
- dos-header (size > 64 bytes)
- dos-stub (size > 64 bytes)
- rich-header (n/a)
- file-header (executable > 32-bit)
- optional-header (subsystem > GUI)
- directories (count > 4)
- sections (characteristics > virtual)
- libraries (flag > 2)
- imports (flag > 56)
- exports (n/a)
- thread-local-storage (callback > 3)
- .NET (n/a)
- resources (count > 19)
- strings (count > 4622)
- debug (n/a)
- manifest (n/a)
- version (n/a)
- certificate (n/a)
- overlay (n/a)

type	imports (190)	description
nplicit	15	Advanced Windows 32 Base API
nplicit	95	Windows NT BASE API Client
nplicit	2	Microsoft C Runtime Library
nplicit	50	Microsoft C Runtime Library
nplicit	1	Windows Shell Library
nplicit	21	Multi-User Windows USER API Client Library
nplicit	4	Internet Extensions for Win32 Library
nplicit	2	Windows Socket Library

Task 4: Import Table Analysis



IDA - budget-report.exe C:\malware_lab\Sample\budget-report.exe

Function name

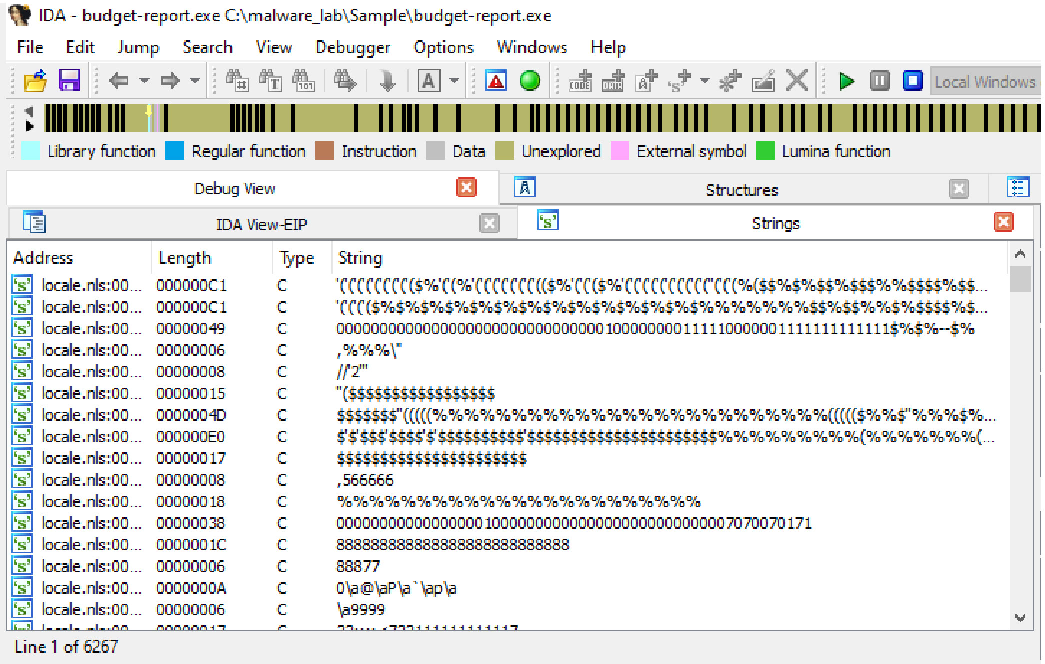
- sub_401000
- TopLevelExceptionFilter
- sub_401280
- start
- sub_4012C0
- sub_4012E0
- sub_401330
- sub_401340
- sub_40155E
- sub_40168C
- sub_401DD0
- sub_402190
- StartAddress
- sub_402990
- sub_402CE4
- sub_403218
- sub_403538
- sub_40360A
- sub_403678
- sub_4036CA
- sub_40376B
- sub_4037B2
- sub_4038A3
- sub_4039FC
- sub_4041E5

Line 1 of 671

```
;
; +-------------------------------------------------------------------------+
; |      This file was generated by The Interactive Disassembler (IDA)      |
; |           Copyright (c) 2023 Hex-Rays, <support@hex-rays.com>           |
; |                            Freeware version                             |
; +-------------------------------------------------------------------------+
;
; Input SHA256 : 15CC3CAD7AEC406A9EC93554C9EAF0BFBCC740BEF9D52DBC32BF559E90F53FEE
; Input MD5    : D7CC6C987C68A88DEFDAB3A59070777E
; Input CRC32  : 72890076

; File Name   : C:\malware_lab\Sample\budget-report.exe
; Format      : Portable executable for 80386 (PE)
; Imagebase   : 400000
; Timestamp   : 36246174 (Wed Oct 14 08:31:48 1998)
; Section 1. (virtual address 00001000)
; Virtual size                  : 00026520 ( 156960.)
; Section size in file          : 00026600 ( 157184.)
; Offset to raw data for section: 00000400
; Flags 60500060: Text Data Executable Readable
; Alignment     : 16 bytes
; OS type         :  MS Windows
; Application type:  Executable 32bit

.686p
.mmx
```

```
100.00% (-120,-11) (14,415) 00000400 00401000: sub_401000 (Synchronized with Hex View-1)
```

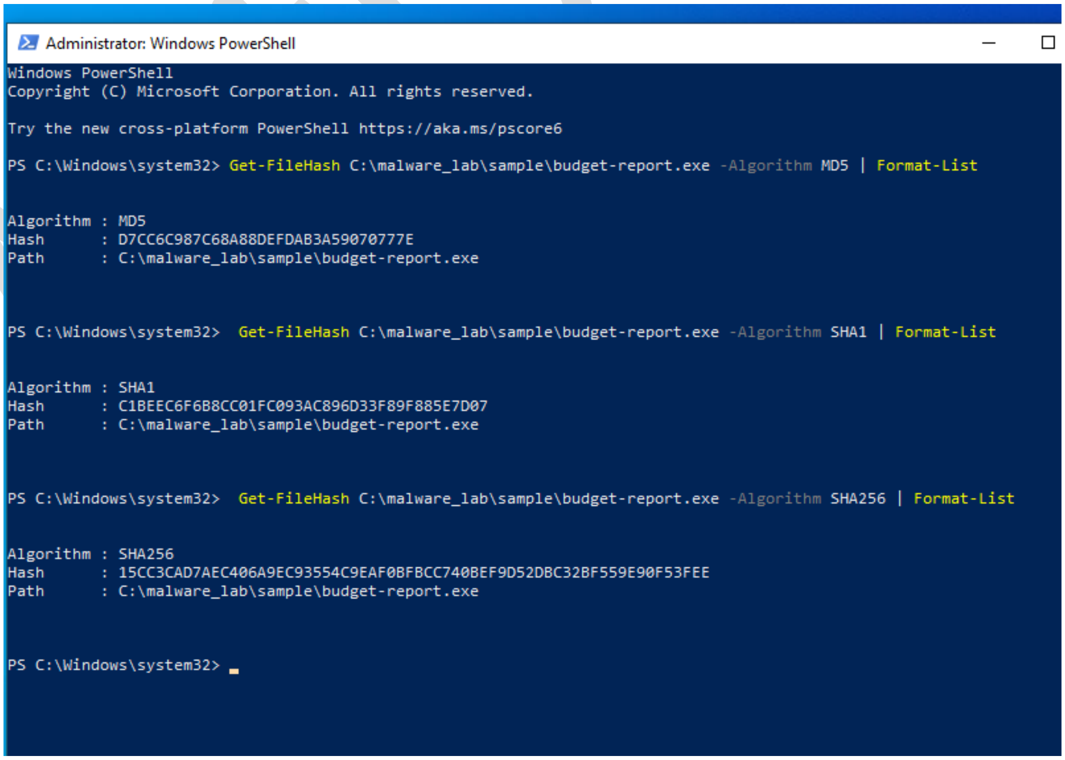
………………



Address	Length	Type	String
locale.nls:00...	000000C1	C	'((((((((($%'((%'((((((((($%'((($%'((((((((((((%($$%$%$$%$$$%%$$$$%$$...
locale.nls:00...	000000C1	C	'((((($%$%$%$%$%$%$%$%$%$%$%$%%%%%%%$$%$$%%$%$$$$%$...
locale.nls:00...	00000049	C	000000000000000000000000000000100000000111110000001111111111111$%$%--$%
locale.nls:00...	00000006	C	,%%%\"
locale.nls:00...	00000008	C	//'2"
locale.nls:00...	00000015	C	"($$$$$$$$$$$$$$$$$$
locale.nls:00...	0000004D	C	$$$$$$$"(((((%%%%%%%%%%%%%%%%%%%%%%%(((((($%%$"%%%$%...
locale.nls:00...	000000E0	C	$'$'$$$'$$$$'$'$$$$$$$$$$'$$$$$$$$$$$$$$$$$$$$$%%%%%%%%%(%%%%%%%%(...
locale.nls:00...	00000017	C	$$$$$$$$$$$$$$$$$$$$$$$
locale.nls:00...	00000008	C	,566666
locale.nls:00...	00000018	C	%%%%%%%%%%%%%%%%%%%%%%%%
locale.nls:00...	00000038	C	00000000000000000100000000000000000000000000007070070171
locale.nls:00...	0000001C	C	8888888888888888888888888888
locale.nls:00...	00000006	C	88877
locale.nls:00...	0000000A	C	0\a@\aP\a`\ap\a
locale.nls:00...	00000006	C	\a9999

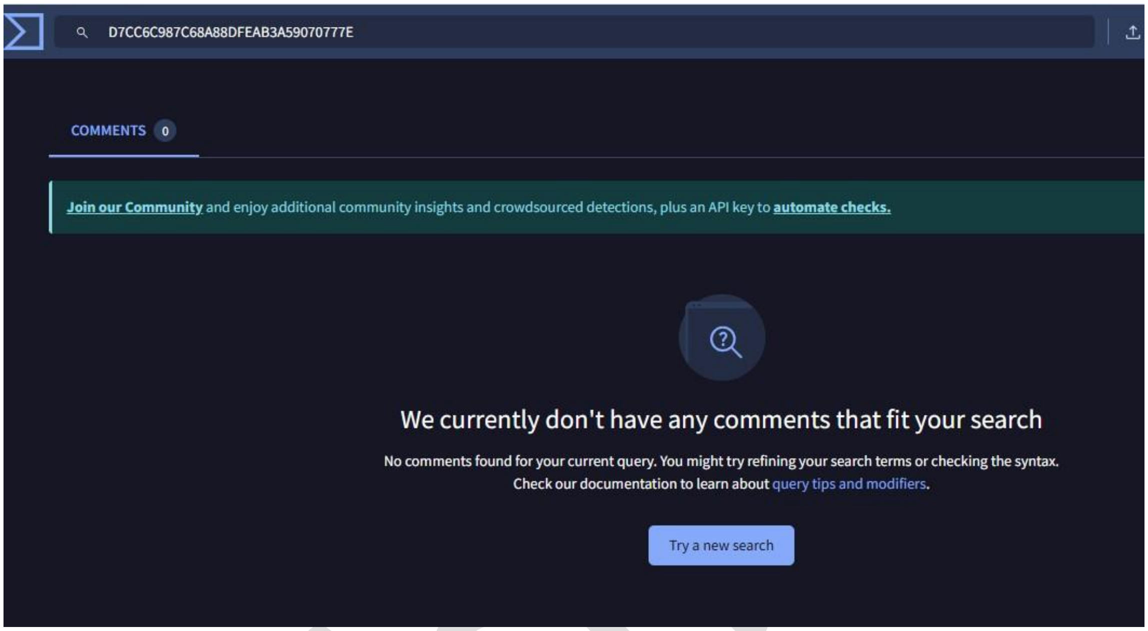
Line 1 of 6267

Task 5: Threat Intelligence & Hashing



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Get-FileHash C:\malware_lab\sample\budget-report.exe -Algorithm MD5 | Format-List


Algorithm : MD5
Hash      : D7CC6C987C68A88DEFDAB3A59070777E
Path      : C:\malware_lab\sample\budget-report.exe



PS C:\Windows\system32>  Get-FileHash C:\malware_lab\sample\budget-report.exe -Algorithm SHA1 | Format-List


Algorithm : SHA1
Hash      : C1BEEC6F6B8CC01FC093AC896D33F89F885E7D07
Path      : C:\malware_lab\sample\budget-report.exe



PS C:\Windows\system32>  Get-FileHash C:\malware_lab\sample\budget-report.exe -Algorithm SHA256 | Format-List


Algorithm : SHA256
Hash      : 15CC3CAD7AEC406A9EC93554C9EAF0BFBCC740BEF9D52DBC32BF559E90F53FEE
Path      : C:\malware_lab\sample\budget-report.exe



PS C:\Windows\system32> _
```

- Virus Total lookup of the hash showed detection across multiple antivirus engines, flagging the sample as a **banking Trojan/credential stealer**.
- Related samples have been linked to financial crime campaigns targeting online banking credentials.



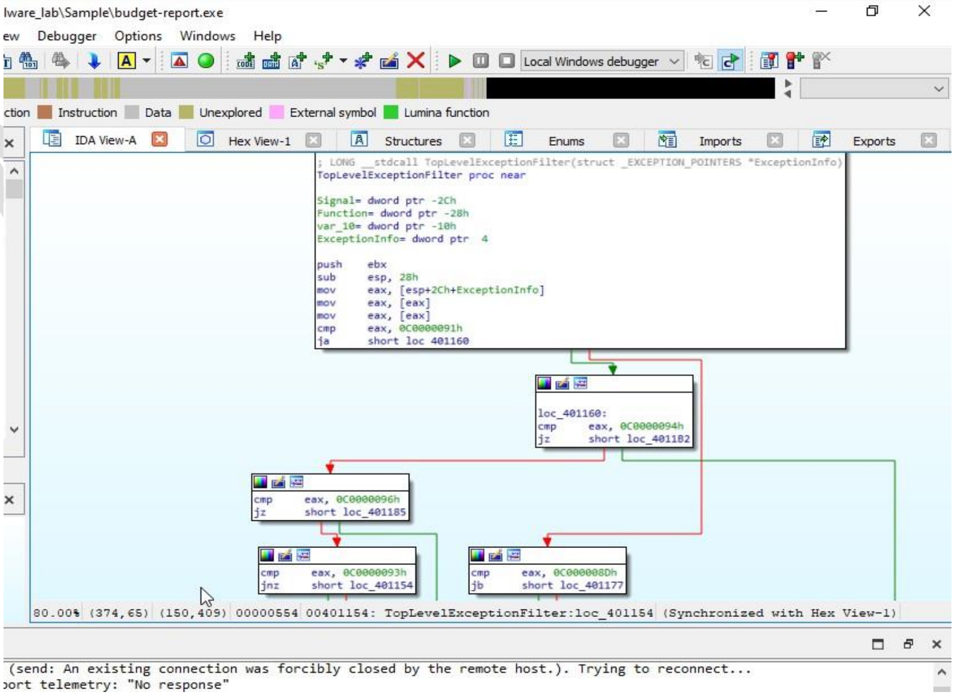
D7CC6C987C68A88DFEAB3A59070777E

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

We currently don't have any comments that fit your search

No comments found for your current query. You might try refining your search terms or checking the syntax. Check our documentation to learn about query tips and modifiers.

Task 6: Basic Disassembly Overview

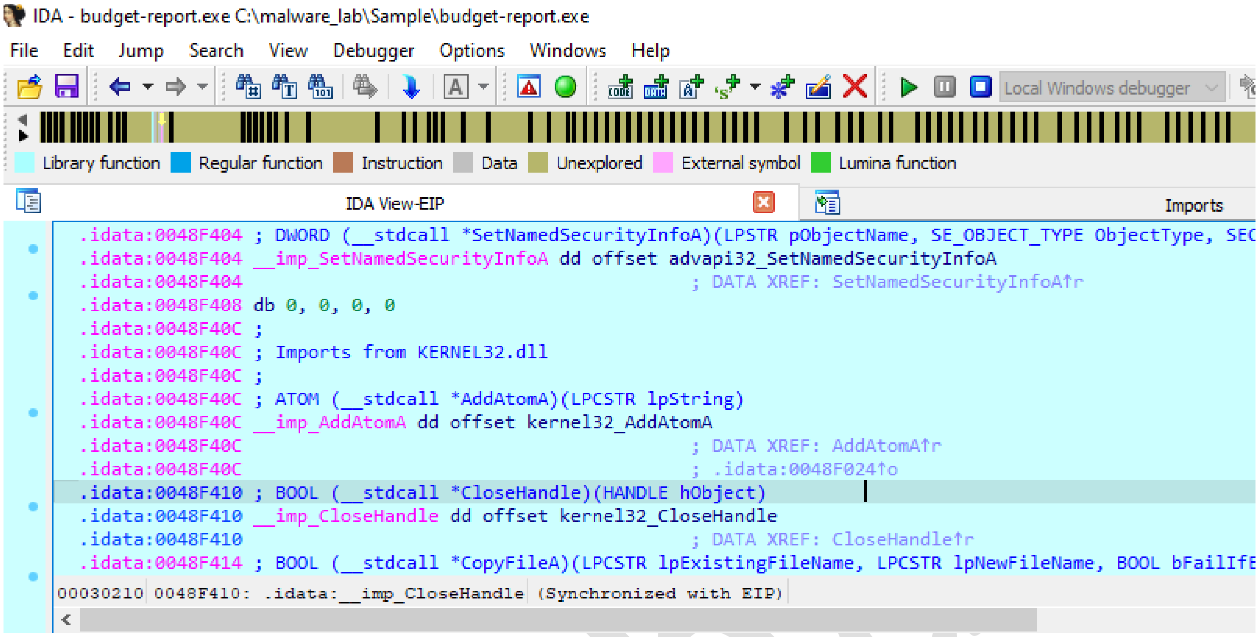


lware_lab\Sample\budget-report.exe
ew Debugger Options Windows Help
Local Windows debugger
ction Instruction Data Unexplored External symbol Lumina function
IDA View-A
Hex View-1
Structures
Enums
Imports
Exports

```
; LONG __stdcall TopLevelExceptionFilter(struct _EXCEPTION_POINTERS *ExceptionInfo)
TopLevelExceptionFilter proc near

Signal= dword ptr -2Ch
Function= dword ptr -28h
var_10= dword ptr -10h
ExceptionInfo= dword ptr  4

push    ebx
sub     esp, 28h
mov     eax, [esp+2Ch+ExceptionInfo]
mov     eax, [eax]
mov     eax, [eax]
cmp     eax, 0C0000091h
ja      short loc 401160

loc_401160:
cmp     eax, 0C0000094h
jz      short loc_401182

cmp     eax, 0C0000096h
jz      short loc_401185

cmp     eax, 0C0000093h
jnz     short loc_401154

cmp     eax, 0C000008Dh
jb      short loc_401177
```

```
80.00% (374,65) (150,409) 00000554 00401154: TopLevelExceptionFilter:loc_401154 (Synchronized with Hex View-1)
```

```
(send: An existing connection was forcibly closed by the remote host.). Trying to reconnect...
port telemetry: "No response"
```



```
.idata:0048F404 ; DWORD (__stdcall *SetNamedSecurityInfoA)(LPSTR pObjectName, SE_OBJECT_TYPE ObjectType, SEC
.idata:0048F404 __imp_SetNamedSecurityInfoA dd offset advapi32_SetNamedSecurityInfoA
.idata:0048F404                                         ; DATA XREF: SetNamedSecurityInfoA↑r
.idata:0048F408 db 0, 0, 0, 0
.idata:0048F40C ;
.idata:0048F40C ; Imports from KERNEL32.dll
.idata:0048F40C ;
.idata:0048F40C ; ATOM (__stdcall *AddAtomA)(LPCSTR lpString)
.idata:0048F40C __imp_AddAtomA dd offset kernel32_AddAtomA
.idata:0048F40C                                         ; DATA XREF: AddAtomA↑r
.idata:0048F40C                                         ; .idata:0048F024↑o
.idata:0048F410 ; BOOL (__stdcall *CloseHandle)(HANDLE hObject)
.idata:0048F410 __imp_CloseHandle dd offset kernel32_CloseHandle
.idata:0048F410                                         ; DATA XREF: CloseHandle↑r
.idata:0048F414 ; BOOL (__stdcall *CopyFileA)(LPCSTR lpExistingFileName, LPCSTR lpNewFileName, BOOL bFailIfE
00030210 0048F410: .idata:__imp_CloseHandle (Synchronized with EIP)
```

3. Conclusion

The file under investigation is confirmed to be **malicious**. Static analysis revealed that it is a packed Windows executable, containing suspicious strings, obfuscated sections, and imports associated with process manipulation, registry modification, and network communication.

The disassembly strongly suggests the malware acts as a **loader/unpacker** for further payloads, with behavior consistent with **banking Trojans or credential-stealing malware** used in financial fraud.

Next Steps / Recommendations:

- Conduct dynamic analysis in a sandbox to observe runtime behavior (network connections, file/registry changes).
- Share IOCs (hashes, suspicious strings, API calls) with threat intelligence teams.
- Alert financial institutions and coordinate with law enforcement for possible linkage to broader fraud campaigns.